PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
G07F 7/08, 7/02

A1

(11) Internationale Veröffentlichungsnummer: WO 96/33475

(43) Internationales Veröffentlichungsdatum: 24. Oktober 1996 (24.10.96)

(21) Internationales Aktenzeichen: PCT/EP96/01521

(22) Internationales Anmeldedatum: 9. April 1996 (09.04.96)

(30) Prioritätsdaten:
95105932.8 20. April 1995 (20.04.95) EP
(34) Länder für die die regionale oder internationale Anmeldung eingereicht worden ist: DE usw.

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D-80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: SCHRENK, Hartmut [DE/DE]; Fasanenweg 22, D-85540 Haar (DE).

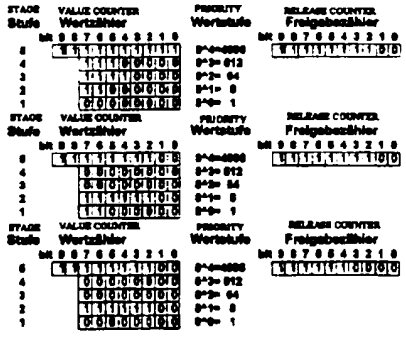
(81) Bestimmungsstaaten: CN, JP, KR, RU, UA, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: ELECTRONIC CREDIT CARD AND PROCESS FOR RELOADING AN ELECTRONIC CREDIT CARD

(54) Bezeichnung: ELEKTRONISCHE BÖRSENKARTE UND VERFAHREN ZUM WIEDERAUFLADEN EINER ELEKTRONISCHEN BÖRSENKARTE

(57) Abstract



An electronic credit card is disclosed, as well as a process for reloading an electronic credit card having an integrated semiconductor circuit that consists of at least one address and control logic circuit and a non-volatile memory with at least one erasable part. The memory addresses of the area of the non-volatile memory in which the value units of the credit card are stored are subdivided into partial zones (stages 1 to 5) of different priorities (orders of priority 1, 8, 64, 512, 4096). Memory addresses may only be erased if all memory addresses of a partial zone having a determined priority are erased at the same time, and each partial zone may only be erased after a carry-over value is written in a previously unwritten memory address of the partial zone having the next higher order or priority. The invention is characterised in that release values stored in a release register of the credit card are associated with the value units of at least the memory addresses of the highest priority partial zone (stage 5). These release values represent a release or a locking state for the associated value stored in the memory addresses of at least the highest priority partial zone. The value stored in the credit card may only be increased after the state of a release value associated with a memory address is changed from a locking state to a release state.

(57) Zusammenfassung

Die Erfindung bezieht sich auf eine elektronische Börsenkarte und ein Verfahren zum Wiederaufladen einer elektronischen Börsenkarte mit einer integrierten Halbleiter-Schaltungsvorrichtung bestehend aus zumindest einer Adreß- und Steuerlogikschaltung und einem nichtflüchtigen Speicher, wobei zumindest ein Teil des nichtflüchtigen Speichers löschbar ist, und die Speicherplätze des zum Speichern der jeweiligen Werteinheiten der Börsenkarte vorgesehenen Bereiches des nichtflüchtigen Speichers in Teilbereiche (Stufen 1 bis 5) jeweils unterschiedlicher Wertigkeit (Stufenwerte 1, 8, 64, 512, 4096) aufgeteilt sind, ein Löschen der Speicherplätze nur für sämtliche Speicherplätze eines Teilbereiches bestimmter Wertigkeit gleichzeitig möglich ist, und jeder Teilbereich nur gelöscht werden kann, nachdem das Einschreiben eines Übertragwertes in einen zuvor unbeschriebenen Speicherplatz des Teilbereiches der nächsthöheren Wertigkeit erfolgt ist. Die Erfindung zeichnet sich dadurch aus, daß den Werteinheiten von zumindest den Speicherplätzen des höchstwertigen Teilbereiches (Stufe 5) in einem Freigaberegister der Börsenkarte zu speichernde Freigabewerte zugeordnet sind, welche entweder einen Freigabe- oder einen Sperrzustand für den jeweils zugeordneten Wertzustand der Speicherplätze des wenigstens höchstwertigen Teilbereiches repräsentieren, und eine Erhöhung des Kartenwertes der Börsenkarte lediglich durch Änderung eines dem Wertzustand eines Speicherplatzes zugeordneten Freigabewertes vom Sperr- in einen Freigabezustand ermöglicht wird.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AM	Armenien	GB	Vereinigtes Königreich	MX	Mexiko
AT	Österreich	GE	Georgien	NE	Niger
AU	Australien	GN	Guinea	NL	Niederlande
BB	Barbados	GR	Griechenland	NO	Norwegen
BE	Belgien	HU	Ungarn	NZ	Neuseeland
BF	Burkina Faso	IE	Irland	PL	Polen
BG	Bulgarien	IT	Italien	PT	Portugal
BJ	Benin	JP	Japan	RO	Rumänien
BR	Brasilien	KE	Kenya	RU	Russische Föderation
BY	Belarus	KG	Kirgisistan	SD	Sudan
CA	Kanada	KP	Demokratische Volksrepublik Korea	SE	Schweden
CF	Zentrale Afrikanische Republik	KR	Republik Korea	SG	Singapur
CG	Kongo	KZ	Kasachstan	SI	Slowenien
CH	Schweiz	LI	Liechtenstein	SK	Slowakei
CI	Côte d'Ivoire	LK	Sri Lanka	SN	Senegal
CM	Kamerun	LR	Liberia	SZ	Swasiland
CN	China	LK	Litauen	TD	Tschad
CS	Tschechoslowakei	LU	Luxemburg	TG	Togo
CZ	Tschechische Republik	LV	Lettland	TJ	Tadschikistan
DE	Deutschland	MC	Monaco	TT	Trinidad und Tobago
DK	Dänemark	MD	Republik Moldau	UA	Ukraine
EE	Estland	MG	Madagaskar	UG	Uganda
ES	Spanien	ML	Mali	US	Vereinigte Staaten von Amerika
FI	Finnland	MN	Mongolei	UZ	Usbekistan
FR	Frankreich	MR	Mauretanien	VN	Vietnam
GA	Gabon	MW	Malawi		

Beschreibung

Elektronische Börsenkarte und Verfahren zum Wiederaufladen einer elektronischen Börsenkarte

Die Erfindung bezieht sich auf ein Verfahren zum Wiederaufladen einer elektronischen Börsenkarte für einen bargeldlosen Zahlungsverkehr mit einer integrierten Halbleiter-Schaltungsvorrichtung bestehend aus zumindest einer Adreß- und Steuerlogikschaltung und einem nichtflüchtigen Speicher, wobei zumindest ein Teil des nichtflüchtigen Speichers löschbar ist, und die Speicherplätze des zum Speichern der jeweiligen Werteinheiten der Börsenkarte vorgesehenen Bereiches des nichtflüchtigen Speichers in Teilbereiche jeweils unterschiedlicher Wertigkeit aufgeteilt sind, wobei ein Löschen der Speicherplätze nur für sämtliche Speicherplätze eines Teilbereiches bestimmter Wertigkeit gleichzeitig möglich ist, und jeder Teilbereich nur gelöscht werden kann, nachdem das Einschreiben eines Übertragwertes in einen zuvor unbeschriebenen Speicherplatz des Teilbereiches der nächsthöheren Wertigkeit erfolgt ist, und bezieht sich auf eine elektronische Börsenkarte für einen bargeldlosen Zahlungsverkehr mit einer integrierten Halbleiter-Schaltungsvorrichtung zur Durchführung des Verfahrens.

Zum bargeldlosen Bezahlen von Waren oder zum Abrechnen von Dienstleistungen und dergleichen sind datengesteuerte Zahlungssysteme in Form von Datenaustauschsystemen bekannt, bei denen die hierbei verwendeten Börsenkarten als ein wesentliches Element einen nichtflüchtigen elektronischen Datenspeicher enthalten, auf den über elektrische Kontakte an der Kartenoberfläche zugegriffen werden kann. Über eine Dateneinbzw. Datenausgabeeinrichtung (Verkaufsterminal) wird von einer Recheneinheit bei jedem Gebrauch auf den Speicherinhalt zugegriffen, der dabei gegebenenfalls geändert wird. Speziell bei der Verwendung von vorausbezahlten Datenträgeranordnun-

gen, die eine anonyme Bezahlung von Waren oder gebührenpflichtigen Diensten ermöglichen, muß sichergestellt sein, daß der Wert der Karte durch Manipulation nur verringert, nicht aber erhöht werden kann.

Wiederaufladbare Börsenkarten sind bisher vorwiegend als Prozessorkarten realisiert worden, da die höhere Rechenleistung eines Mikroprozessors eine Kontrolle der Wiederaufladung vereinfachte. In Lowend-Zahlungssystemen finden jedoch, insbesondere bei vorausbezahlten Karten, zunehmend intelligente Speicherkarten Verwendung. Die von der Anmelderin derzeit verwendete Chipkarte zeigt, daß kryptologische Echtheits- und Berechtigungsprüfungen der Teilnehmer an Zahlungsvorgängen heute auch mit Speicherchips auf vergleichbarem Sicherheitsniveau realisierbar sind. Die elektronische Überwachung der übertragenen Geldbeträge mit den über Mikroprozessoren realisierten Verfahren würden jedoch solche Karten zu aufwendig machen.

Bei wiederaufladbaren Börsenkarten, sowohl auf Mikroprozessor-, als auch auf Speicherbasis, ist grundsätzlich davon auszugehen, daß nicht nur ein Systemgeheimnis, sondern auch ein Kryptoalgorithmus für Echtheitsprüfungen vorhanden ist. Trotzdem sind verschiedene Risiken zu betrachten. Zum einen kann auch nach elektronischer Authentifikation der am Wiederaufladen beteiligten Partner nicht ausgeschlossen werden, daß ein Betrüger durch Manipulation der Übertragungsdaten den Aufbuchungswert der Börsenkarte manipuliert. Zum weiteren besteht die Aufbuchung aus einem Lösch-Schreibzyklus des nichtflüchtigen Zählbereichs, bei dem die Börsenkarte vorübergehend auch einen höheren Geldwert annehmen kann. Eine Unterbrechung des Ladevorgangs in einem geeigneten Augenblick würde dann zu einem unberechtigt hohen Börsenwert führen. Ein Lösch-Schreibzyklus setzt sich hierbei aus zwei Vorgängen zusammen: zuerst Löschen des vollgeschriebenen Zählers oder von Teilbereichen des Zählers, und danach Einstellung bzw. Einschreiben des neuen Zählerstandes. Löschen ist hierbei

definitionsgemäß der Vorgang, bei dem eine größere Anzahl von Informationswerten (Bits) auf Speicherplätzen gleichsinnig geändert wird. Erst durch Schreiben wird anschließend das gewünschte spezifische Bitmuster erzeugt. Entwerten durch Schreiben einzelner Bits muß aus sicherheitstechnischen Gründen der elektrische Entladevorgang von Speicherplätzen sein, damit bei eventueller Selbstentladung der Zellen der Börsenwert nur abnehmen kann. Löschen ist damit der risikobehaftete, werterhöhende Vorgang. Im Zeitraum zwischen dem Löschen und dem Schreiben nimmt der Zähler als Zwischenzustand vorübergehend einen Maximalwert an, der erst durch die Schreibvorgänge wieder korrigiert wird. Das Manipulationsrisiko bei der bekannten Chipkarte liegt in diesem unvermeidbaren Zwischenzustand.

Gemäß der schematischen Darstellung nach Fig. 1 soll zunächst das Funktionsprinzip einer heutigen, vorbezahlten Karte, die nach einem vollständigen Verbrauch des Börsenwertes nicht erneuert wird, erläutert werden. Der Abbuchvorgang beispielsweise in einer vorbezahlten Telefon-Wertkarte wird in der Regel mit einem Sicherheitszähler als "elektronischer Abakus" realisiert, beispielsweise durch das in der EP 0 321 727 B1 beschriebene Verfahren. Ein nichtflüchtiger Wertzähler ist in der Weise elektronisch abgesichert, daß sein Wert durch die Programmiervorgänge niemals erhöht werden kann. Konventionelle Binärzähler, bei denen fortlaufend Bits gelöscht und geschrieben werden müssen, scheiden als Wertzähler aus.

Gemäß Fig. 1 besteht die in der Karte verwendete Zählanordnung aus einem Wertzähler mit fünf Stufen zu je 8 EEPROM-Zellen, die als Oktalzähler verschaltet sind. Jeder Stufe ist eine festgelegte Wertigkeit zugeordnet. Im Oktalzähler hat in benachbarten Wertstufen ein Bit der höherwertigen Stufe jeweils die 8-fache Wertigkeit eines Bits der darunter liegenden Stufe. In Telefonkarten sind den Bits der fünf 8-Bit-Stufen jeweils die Werteinheiten 1, 8, 64, 512 bzw. 4096 zugeordnet. Bei dem Zahlenbeispiel gemäß Fig. 1 wird bei-

spielsweise bei der Initialisierung einer 12-DM-Karte (= 1.200 Werteinheiten) ein entsprechender Zählerstand eingestellt (1.200 = 2*512 + 2*64 + 6*8). Der theoretische, maximale Zählumfang der Karte von 8^5 = 32768 Einheiten wird in der Regel nicht ausgenützt, im angegebenen Beispiel befindet sich daher kein einziges Bit in der obersten Zählstufe 5. Vor der Entwertung sind die Zählerbits gelöscht und haben gemäß der vorliegend verwendeten Definition den logischen Zustand "1". Zur Entwertung wird der fällige Betrag auf die fünf Zählerstufen aufgeteilt und die betreffende Anzahl von Bits durch Schreiben von "1" nach "0" entwertet. Die unteren vier Wertstufen 1 bis 4 sind als EEPROM, die oberste Stufe 5 ist als PROM ausgebildet. Sind alle Bits einer unteren Wertstufe verbraucht, so muß über das Terminal vor weiteren Abbuchungen ein interner Umbuchvorgang eingeschoben werden, bei dem die 8 vollgeschriebenen Bits einer Stufe wieder nach "1" gelöscht werden, nachdem zuvor ein gelöschtes Bit der darüberliegenden Stufe durch Schreiben nach "0" entwertet worden ist. Der Umbuchvorgang selbst ist wertneutral, da sich Entwertung und Aufwertung ausgleichen. Für eine absichtliche Unterbrechung des Umbuchvorgangs gibt es keinen Betrugsanreiz, da die Entwertung zuerst vorgenommen wird. Der Zählerstand der Telefonkarte kann vom vorgegebenen Anfangswert mittels Schreib- und Löschvorgängen nur herabgesetzt werden und ist damit vom Konzept her schwer manipulierbar.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren bzw. eine Vorrichtung zur Verfügung zu stellen, welche mit einem vergleichsweise geringen Zusatzaufwand eine manipuliersichere Wiederaufladung mit einem beliebigen Börsenwert ermöglicht, wobei gleichzeitig die derzeit verwendeten Konzepte von Chipkarten im wesentlichen beibehalten werden sollen.

Diese Aufgabe wird durch ein Verfahren zum Wiederaufladen einer Börsenkarte mit einer Halbleiter-Schaltungsvorrichtung gemäß Anspruch 1 und durch eine im Anspruch 9 angegebene Börsenkarte gelöst.

Der Erfindung liegt zunächst die Erkenntis zugrunde, daß neue Werteinheiten auf der Börsenkarte tatsächlich nicht im physikalischem Sinne neu geladen werden, sondern durch Einführung eines unabhängig zu schreibenden Freigabewertes lediglich freigegeben werden. Auf diese Weise wird unter Beibehaltung der wesentlichen Konzepte der bisherig verwendeten Speicherkarten eine manipulationsgeschützte Wiederaufladung möglich, und zwar mit einem lediglich geringen Zusatzaufwand. Die Börsenkarte erreicht in der Phase der Freigabe zu keinem Zeitpunkt einen erhöhten Geldwert. Das Konzept der gesicherten internen Umladung des Sicherheitszählers wird auch für die Wiederaufladung mit genutzt. Der kritische Vorgang des Löschens wird im Rahmen der eigentlichen Wiederaufladung gar nicht durchgeführt und aus der Aufladung ausgegliedert. Während einer Wiederaufladung wird nur geschrieben.

Dem Prinzip der Erfindung folgend wird der Wertzähler der Börsenkarte in der aufladbaren elektronischen Börsenkarte im Zählumfang durch zumindest ein Freigaberegister in der Weise erweitert, daß er die Summe aller möglichen Aufladungen bestimmt. Für das zusätzlich in der Börsenkarte vorgesehene Freigaberegister sind nicht übermäßig viele zusätzliche Speicherplätze erforderlich, da es sich zunächst lediglich um die höchstwertigen Bits im Wertzähler handelt, die einzeln jeweils viele Werteinheiten beinhalten. Im Aufladeterminal werden die Werteinheiten des vergrößerten Wertzählers durch Schreiboperationen für die Abbuchung erst freigegeben oder, anders ausgedrückt, im Wertzähler aufgebucht. Die freigegebenen Werteinheiten erlauben anschließend die Durchführung wertneutraler Umbuchvorgänge innerhalb des Wertzählers, die erst im Verkaufsterminal im Rahmen einer Abbuchung veranlaßt werden, und die erprobte Manipuliersicherheit des Sicherheitszählers in der Börsenkarte ohne zusätzliches Risiko ausnützen.

Erfindungsgemäß sind den Werteinheiten von zumindest den Speicherplätzen des höchstwertigen Teilbereiches in dem Freigaberegister der Börsenkarte zu speichernde Freigabewerte zugeordnet, welche entweder einen Freigabe- oder einen Sperrzustand für die jeweils zugeordneten Werteinheiten der Speicherplätze des wenigstens höchstwertigen Teilbereiches repräsentieren. Eine Erhöhung des Kartenwertes der Börsenkarte ist lediglich durch Änderung eines der Werteinheit eines Speicherplatzes zugeordneten Freigabewertes vom Sperr- in einen Freigabezustand möglich.

Hierbei kann bei einer bevorzugten Ausführung der Erfindung vorgesehen sein, daß die aufgrund des im Freigaberegister geschriebenen Freigabewertes ermöglichte Freigabe einer zugeordneten Werteinheit in dem Teilbereich der Speicherplätze einer bestimmten Wertigkeit zum Löschen des Teilbereiches der nächstniedrigeren Wertigkeit verwendet wird. Die Wiederaufladung der Börsenkarte wird hierbei durch einen Schreibvorgang von einem oder mehreren Freigabewerten im Freigaberegister zur Freigabe der zugeordneten Werteinheiten in einem Teilbereich des Speichers ausgeführt.

In bevorzugter Weise wird das Schreiben einer Werteinheit in einem Teilbereich des Speichers und damit der Verbrauch eines nachzuladenen Geldwertes erst dann ermöglicht, nachdem ein zugeordneter Freigabewert im Freigaberegister geschrieben worden ist.

Bei einer konkreten Ausgestaltung bzw. Durchführung des erfindungsgemäßen Verfahrens ist vorgesehen, daß die Aufladung der Börsenkarte in einem Ladeterminal in vorbestimmten Schrittweiten oder deren Vielfachen entsprechend der Wertigkeit der bezüglich der höchstwertigen Wertstufe unmittelbar darunterliegenden und zu löschenden Wertstufe durchgeführt wird.

Bei einer weiterhin bevorzugten Ausführung der Erfindung kann vorgesehen sein, daß der sicherheitsrelevante Ladevorgang der Börsenkarte nur wertmindernde Schreibvorgänge oder wertneutrale Umbuchungen beinhaltet, und vor einer Freigabe einer Werteinheit eine Echtheitsprüfung der Börsenkarte im Ladeterminal vorgenommen wird. Das Verkaufsterminal sendet dabei an die Börsenkarte eine frei wählbare Challenge und dazu die unter Kenntnis eines gemeinsamen Geheimnisses berechnete Response. Die Börsenkarte vergleicht intern die vom Verkaufsterminal gesendete Response mit dem selbsterrechneten Wert. Bei Übereinstimmung wird durch chipinterne Logik ohne zusätzliche externe Datenübertragung jeweils ein Bit im Freigaberegister freigegeben. Eine externe Einflußmöglichkeit auf den Aufladebetrag besteht nicht. Bei Übereinstimmung wird durch chipinterne Logik ohne zusätzliche externe Datenübertragung jeweils ein Bit im Freigaberegister freigegeben. Eine externe Einflußmöglichkeit auf den Aufladebetrag besteht nicht. Die gesamte Sicherheitsüberprüfung beim Wiederaufladen läßt sich durch (gegenseitige) Authentifikation mittels einer zuverlässigen kryptologischen Einwegfunktion absichern.

Der sicherheitskritische Löschvorgang des Ladens ist als Umbuchungsvorgang in den Abbuchungsvorgang am Verkaufsterminal integriert. Die Übernahme eines Restwertes der Börsenkarte vom Zustand vor der Aufladung ergibt sich durch das Konzept von selbst, weil die freigegebenen Einheiten im Wertzähler zum bisherigen Stand des Wertzählers ohne Zusatzaufwand hinzuaddiert werden.

Bei einer Ausführung der Erfindung kann der Gesamtkartenwert durch die Aufladung durch den Wert eines Bits im Freigaberegister auf einen Mindestwert festgelegt sein. Die manipuliergeschützte Aufladung um beliebig einstellbare, größere Geldwerte ist hierbei erst ab Freigabe von zwei Bits im Freigaberegister möglich, weil nur dann unter allen Restwertbedingungen die erforderlichen Umladungen im Wertzähler unter Benutzung eines ersten Freigabebits durchführbar sind und gleich-

zeitig die Karte sich dabei noch in einem niederwertigen Zustand befindet.

Sind die Ladewerte kleiner als zwei Wertbits im Freigaberegister, kann es passieren, daß der Wertausgleich im Wertzähler bei nur einem Freigabebit erst nach der Freigabe des Bits im Freigaberegister durchgeführt werden kann und damit weniger geschützt ist. Ein Betrüger könnte dann theoretisch die Börsenkarte vor Abschluß des Wertausgleichs mit Vorteil aus dem Ladeterminal entfernen. Dieses Betrugsrisiko bei kleineren Aufladebeträgen kann durch ein zusätzliches, nichtflüchtiges Backup-Bit innerhalb der Börsenlogik der Börsenkarte beseitigt werden, welches analog zu einer Backup-Logik im Wertzähler der Börsenkarte arbeitet: Es wird beispielsweise gleichzeitig mit dem Freigabebit geschrieben. Zurückgesetzt wird es über das Ladeterminal nach Abschluß des Entwertungsvorganges durch eine Sicherheitsprozedur ähnlich zu der beim Schreiben eines Freigabebits. Im Falle eines betrügerischen Abbruchs bleibt das Backup-Bit gesetzt, so daß diese Börsenkarte durch routinemäßige Überprüfung im Verkaufsterminal auf jeden Fall erkannt und abgewiesen wird.

Sollen sehr viele, kleine Aufladebeträge zugelassen werden, kann es notwendig sein, den Wertzähler so zu konfigurieren, daß der Kontrollbereichanteil am Wertzähler vergrößert und der übrige Wertspeicher entsprechend verkleinert ist. In jedem Fall setzt aber die uneingeschränkte gesicherte Einstellung beliebiger Aufladebeträge immer einen Mindest-Aufladebetrag entsprechend zweier Bits im Freigaberegister voraus. Die maximale Werterhöhung je Aufladung ist dagegen bei dieser Zählerkonfiguration in vorteilhafter Weise nicht eingeschränkt.

Wenn das gesamte Zählvolumen des Wertzählers auf sehr viele, kleine Aufladeeinheiten verteilt werden soll, die dafür sehr häufig aufzuladen sind, könnte der Kontrollbereich und der zugordnete Freigabebereich auch selber wieder als (Oktal-)

Zähler ausgelegt werden. In diesem Fall unterliegt jedoch auch der Maximalbetrag, der bei einem einzigen Ladevorgang durch Schreiben mehrerer Freigabebits im Wertzähler freigegeben werden kann, zusätzlichen Einschränkungen. Bei wertneutralen Umladungen innerhalb der oberen Zählbereiche kann nämlich die direkte Zuordnung der Bits im Freigaberegister (geändert im Ladeterminal) und im Wertzähler (geändert im Verkaufsterminal) verloren gehen, so daß der Börseninhaber tatsächlich nicht den vollen Aufladewert verbrauchen kann. Diese Einschränkungen im maximalen Betrag bei einem einzigen Aufladevorgang können wiederum durch eine zusätzliche Flagsteuerung beseitigt werden, wobei diese Zählkonfiguration im wesentlichen nur für spezielle Zählanforderungen interessant sein dürfte.

Bei einer bevorzugten Ausgestaltung einer erfindungsgemäßen Börsenkarte kann vorgesehen sein, daß vor der Entwertung eines Bits im Kontrollbereich des Wertzählers chipintern nicht nur geprüft wird, ob das Zusatzbit noch gelöscht "1" ist, sondern auch ob das zugeordnete Freigabebit den Freigabezustand "0" besitzt. Hierbei kann bei einer einfachen Ausgestaltung vorgesehen sein, daß den beiden Speicherbereichen unabhängige Ausleseschaltungen mit getrennten Spaltendekodern zugeordnet sind, um eine vergleichsweise komplizierte serielle Abfrage beider Zähler zu vermeiden. Es ist außerdem sinnvoll, Wertzähler inklusive Kontrollbereich einerseits und Freigaberegister andererseits mit einer unterschiedlichen Bewertungsspannung am Steuergate der Speicherzellen zu betreiben. Wie bereits erwähnt, muß der Wertzähler in der Weise ausgelegt sein, daß der entladene Zustand der EEPROM-Zellen auch dem neutralen, geschriebenen und entwerteten Zustand entspricht. Das Schreiben im Freigaberegister ist dagegen nicht entwertend, sondern werterhöhend. Er ist deshalb durch Wahl einer niedrigeren Gatespannung vorteilhaft in der Weise auszulegen, daß eine Speicherzelle, die durch einen Stress in den Neutralzustand zurückgefallen ist, als "1 " oder nicht freigegeben bewertet wird (d.h. die verwendete Definition von

gelöscht = logisch "1" wird in vorteilhafter Weise beibehalten).

Die Erfindung ist in der nachfolgenden Beschreibung anhand eines in der Zeichnung dargestellten Ausführungsbeispieles im einzelnen beschrieben.

In der Zeichnung zeigt

Fig. 1 das Grundprinzip eines Sicherheitszählers in einer herkömmlichen Speicherkarte,

Fig. 2 das Prinzip der Aufladung durch Freigabe von Restbeträgen mit Restwertübernahme gemäß der Erfindung, und

Fig. 3 die Aufladung mit Freigabe und Umladung des Wertzählers bei einer Wiederaufladung der Börsenkarte mit 10000 Werteinheiten.

Fig. 2 zeigt ein Ausführungsbeispiel der Erfindung, bei dem die Speicherplätze des zum Speichern der jeweiligen Werteinheiten der Börsenkarte vorgesehenen Bereiches des nichtflüchtigen Speichers in Teilbereiche (Stufen 1 bis 5) jeweils unterschiedlicher Wertigkeit (Stufenwerte 1, 8, 64, 512, 4096) aufgeteilt sind, ein Löschen der Speicherplätze nur für sämtliche Speicherplätze eines Teilbereiches bestimmter Wertigkeit gleichzeitig möglich ist, und jeder Teilbereich nur gelöscht werden kann, nachdem das Einschreiben eines Übertragwertes in einen zuvor unbeschriebenen Speicherplatz des Teilbereiches der nächsthöheren Wertigkeit erfolgt ist. Erfindungsgemäß sind den Werteinheiten von zumindest den Speicherplätzen des höchstwertigen Teilbereiches (Stufe 5) in einem Freigaberegister der Börsenkarte zu speichernde Freigabewerte zugeordnet, welche entweder einen Freigabe- ("0") oder einen Sperrzustand ("1") für den jeweils zugeordneten Wertzustand der Speicherplätze des wenigstens höchstwertigen Teilbereiches repräsentieren, und eine Erhöhung des Kartenwertes der

Börsenkarte lediglich durch Änderung eines dem Wertzustand eines Speicherplatzes zugeordneten Freigabewertes vom Sperr- in einen Freigabezustand ermöglicht wird. Bei dem Zahlenbeispiel gemäß Fig. 2 wird beispielsweise bei der Initialisierung einer 100-DM-Karte (= 10.000 Werteinheiten) ein entsprechender Zählerstand eingestellt (10.000 = 2*4096 + 3*512 + 4*64 + 2*8), wobei von den 8 geschriebenen Bits im Wertzähler der obersten Stufe 5 aufgrund der geschriebenen Bits im Freigaberegister lediglich 2 Bits freigegeben werden. In der wiederaufladbaren Börsenkarte ändert sich das prinzipielle Zählprinzip der vorbekannten Telefonkarten nicht, wie im folgenden näher erläutert wird. Die oberste Zählstufe 5 des Wertzählers kontrolliert als PROM wieder das Aufladen der benachbarten Stufe 4 usw. Sie erhält jetzt aber innerhalb des Wertzählers die Zusatzfunktion als Kontrollbereich für Wiederaufladungen. Unter Wiederaufladung wird im folgenden die Freigabe eines oder mehrerer Speicherbits im Kontrollbereich zum Löschen der darunter liegenden Wertstufe 4 verstanden. Die Größe des Kontrollbereichs begrenzt die Summe aller für die Karte erlaubten Zahlungsvorgänge einschließlich der Aufladungen. Im Ausführungsbeispiel können bei einer Größe von 10 Bit beispielsweise insgesamt maximal 10*4096 = 40960 Werteinheiten oder über 400 DM nachgeladen werden. Sollte eine erweiterte Geldbörsenanwendung einschließlich Aufladungen mehr Zähleinheiten erfordern, läßt sich der Kontrollbereich auch als zusätzliche, höchstwertige sechste Zählerstufe ausführen. Der kumulierte Zählumfang steigt dann auf über 300.000. Für Geldbörsen kommt darüber hinaus auch eine andere Ausführung des Sicherheitszählers als die des beschriebenen Oktalzählers in Frage.

Dem Kontrollbereich im Wertzähler, d.h. der obersten Stufe 5 des Wertzählers ist ein gleich aufgebautes Duplikat als Freigaberegister zugeordnet bzw. vorgeschaltet. Das Schreiben eines Bits im Kontrollbereich und damit der Verbrauch eines nachzuladenden Geldwertes ist erst möglich, nachdem das zugeordnete Bit im Freigaberegister geschrieben worden ist. Der

Aufladevorgang der Börsenkarte in einem Ladeterminal besteht aus Schreibvorgängen von einem oder mehreren Bits im Freigaberegister zur Freigabe der zugeordneten Bits im Kontrollzählerbereich. Die Aufladung erfolgt also in festen Schritten oder deren Vielfachen entsprechend dem Wert der unmittelbar darunterliegenden und zu löschenden Wertstufe 4. Der Inhaber der Börsenkarte wird jeweils beim Schreiben der Freigabebits mit dem zugeordneten Geldwert belastet.

Im folgenden soll ein konkretes Zahlenbeispiel für eine Aufladung der Börsenkarte durch Freigabe mit Umbuchung von Festbeträgen gemäß Fig. 2.1 bis 2.3 erläutert werden. Der Kontrollbereich des Wertzählers ist im Beispiel zur Erhöhung des kumulierten Zählumfangs von 8 auf 10 Bit erhöht. Rechts neben dem Kontrollbereich ist der zugeordnete Freigabebereich dargestellt. Fig. 2.1 zeigt den Zustand von Wertspeicher und Freigaberegister bei der Ausgabe der Börsenkarte mit 10 000 Werteinheiten. Diese Werteiheiten setzen sich aus zwei Anteilen zusammen: einem Anteil von 2*4096 Einheiten, die im Kontrollbereich des Wertzählers durch die zwei geschriebenen Bits im Freigaberegister freigegeben sind, und aus einem Anteil von 1808 Einheiten, die sich über den Zustand "1" im Wertzähler auf die Wertstufen 2, 3 und 4 verteilen (= 3*512 + 4*64 + 2*8).

Fig. 2.2 zeigt die gleiche Karte, nachdem sich der Kartenwert auf einen Restwert von 50 Einheiten (entsprechend 50 Pfennig) verringert hat (6*8 + 2). Beim Aufladevorgang werden zwei weitere Bits im Freigaberegister geschrieben und damit im Kontrollbereich des Wertzählers freigegeben. Der Wert der Börsenkarte hat sich dadurch auf 2*4096 + 50 = 8242 Einheiten erhöht.

Die Aufladung der Karte durch Freigabe und Umbuchung frei wählbarer Beträge, sowie ein Wertausgleich im Wertzähler der Börsenkarte wird wie folgt durchgeführt. Ein Merkmal des bisher beschriebenen Aufladekonzeptes ist hierbei, daß die Auf-

ladung nicht in frei wählbaren Schritten sondern nur in Stufen entsprechend dem Wert der zweitobersten Wertstufe 4 erfolgt. Diese Einschränkung läßt sich jedoch in gewissen Grenzen umgehen, wenn man auch den Wertzähler selbst manipulationsgesichert in den Aufladevorgang einbezieht, vgl. Fig. 3. Wenn beispielsweise die letzte Umbucheinheit den Wert des Wertzählers über den gewünschten Aufladebetrag hinaus erhöhen würde, kann die Differenz vor dem Schreiben des letzten Freigabebits durch Schreiben im Wertspeicher ausgeglichen werden. Reicht der im Wertzähler verbliebene Restwert dazu nicht aus, so kann über das Verkaufsterminal auch ein wertneutraler Umbuchvorgang im Wertzähler unter Verwendung des schon freigegebenen Bits im Kontrollbereich veranlaßt werden.

Ein Wertausgleich während des Aufladens durch Schreiben im Wertzähler stellt kein Betrugsrisiko dar, wenn er vor dem Schreiben des letzten Freigabebits stattfindet. Ein Betrüger, der während der Schreibphase den Vorgang absichtlich unterbrechen oder unterdrücken würde, hätte dadurch nur einen Wertverlust durch den fehlenden Betrag des Freigabebits. Eventuelle Manipulation durch Unterdrückung der in den Wertzähler einzuschreibenden Ausgleichsdaten ist vom Terminal erkennbar, wenn der Wertzähler vor der abschließenden Freigabe des letzten Freigabebits noch einmal überprüft wird. Durch gegenseitige Authentifikation wird vor der Freigabe des letzten Bits der Börsenchip mit seinem aktuellen Wertzählerstand durch das Ladeterminal authentifiziert. Die korrekte Chip-Response ist damit auch eine Signatur des aktuellen Zählerstandes. Ist diese Response falsch, so kann der Schreibvorgang im Freigaberegister unterdrückt werden. Ein Betrüger hätte dann nur einen Wertverlust zu tragen.

Im folgenden soll ein konkretes Zahlenbeispiel für die Karte mit einer Aufladung und einer Umbuchung frei wählbarer Beträge erläutert werden. Fig. 3.1 zeigt den Zustand der Börsenkarte von Fig. 2 mit einem Restwert von 50 Einheiten. Diese Karte soll um 10 000 Einheiten oder 100 DM bei Übernahme des

Restwertes manipuliersicher aufgeladen werden. Drei Bits im Freigaberegister würden eine Werterhöhung um 3*4096 = 12288 bedeuten, d.h. 2288 Einheiten zuviel. Ohne Betrugsmöglichkeit werden zunächst 2*4096 Einheiten über den Freigaberegister freigegeben und damit der Kartenwert auf 8242 inklusive Restwert erhöht (Fig. 3.2). Als nächstes wird der Überzahlungsanteil von 2288 = 2*512 + 3*64 + 6*8 Einheiten vor Freigabe des 3. Bits im Freigaberegister vom Wertzähler subtrahiert. Dieser Vorgang besteht im angegebenen Beispiel aus zwei Schritten. Im ersten Schritt wird wertneutral eines der freigegebenen Bits zur Umladung der Wertstufen 4 bzw. 3 verwendet (Fig. 3.3). Von den nunmehr gefüllten Wertzählerstufen wird im zweiten Schritt der Überzahlungsanteil abgebucht. Der Kartenwert geht dabei vorrübergehend auf 5952 Einheiten zurück (Fig. 3.4). Erst mit dem Schreiben des 3. Freigabebits erreicht die Börsenkarte den vorgesehenen Sollwert von 10050 Einheiten und der Ladevorgang ist abgeschlossen.

Patentansprüche

1. Verfahren zum Wiederaufladen einer elektronischen Börsenkarte für einen bargeldlosen Zahlungsverkehr mit einer integrierten Halbleiter-Schaltungsvorrichtung bestehend aus zumindest einer Adreß- und Steuerlogikschaltung und einem nichtflüchtigen Speicher, wobei zumindest ein Teil des nichtflüchtigen Speichers löschbar ist, und die Speicherplätze des zum Speichern der jeweiligen Werteinheiten der Börsenkarte vorgesehenen Bereiches des nichtflüchtigen Speichers in Teilbereiche (Stufen 1 bis 5) jeweils unterschiedlicher Wertigkeit (Stufenwerte 1, 8, 64, 512, 4096) aufgeteilt ist, wobei ein Löschen der Speicherplätze nur für sämtliche Speicherplätze eines Teilbereiches bestimmter Wertigkeit gleichzeitig möglich ist, und jeder Teilbereich nur gelöscht werden kann, nachdem das Einschreiben eines Übertragwertes in einen zuvor unbeschriebenen Speicherplatz des Teilbereiches der nächsthöheren Wertigkeit erfolgt ist,
dadurch gekennzeichnet, daß
den Werteinheiten wenigstens der Speicherplätze des höchstwertigen Teilbereiches (Stufe 5) in einem Freigaberegister der Börsenkarte zu speichernde Freigabewerte zugeordnet sind, welche entweder einen Freigabe- oder einen Sperrzustand für die jeweils zugeordnete Werteinheit der Speicherplätze des wenigstens höchstwertigen Teilbereiches repräsentieren, und eine Erhöhung des Gesamtwertes der Börsenkarte lediglich durch Änderung eines der Werteinheit eines Speicherplatzes zugeordneten Freigabewertes vom Sperr- in einen Freigabezustand ermöglicht wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß die aufgrund des im Freigaberegister geschriebenen Freigabewertes ermöglichte Freigabe einer zugeordneten Werteinheit in dem Teilbereich der Speicherplätze einer bestimmten Wertigkeit zum Löschen des Teilbereiches der nächstniedrigeren Wertigkeit verwendet wird.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, daß die Wiederaufladung der Börsenkarte durch einen Schreibvorgang von einem oder mehreren Freigabewerten im Freigaberegister zur Freigabe der zugeordneten Werteinheiten in einem Teilbereich des Speichers ausgeführt wird.

4. Verfahren nach Anspruch 1 bis 3, **dadurch gekennzeichnet**, daß das Schreiben einer Werteinheit in einem Teilbereich des Speichers und damit der Verbrauch eines nachzuladenen Geldwertes erst ermöglicht wird, nachdem ein zugeordneter Freigabewert im Freigaberegister geschrieben worden ist.

5. Verfahren nach Anspruch 1 bis 4, **dadurch gekennzeichnet**, daß die Aufladung der Börsenkarte in einem Ladeterminal in vorbestimmten Schrittweiten oder deren Vielfachen entsprechend der Wertigkeit des bezüglich des Teilbereiches höchster Wertigkeit unmittelbar darunterliegenden und zu löschenden Teilbereiches durchgeführt wird.

6. Verfahren nach Anspruch 1 bis 5, **dadurch gekennzeichnet**, daß der sicherheitsrelevante Ladevorgang der Börsenkarte nur wertmindernde Schreibvorgänge oder wertneutrale Umbuchungen beinhaltet, und vor einer Freigabe einer Werteinheit eine Echtheitsprüfung der Börsenkarte im Ladeterminal vorgenommen wird.

7. Verfahren nach Anspruch 1 bis 6, **dadurch gekennzeichnet**, daß ein zusätzliches, nichtflüchtiges Backup-Bit in einem Speicherplatz innerhalb der Börsenkarte gleichzeitig mit einem Freigabewert geschrieben wird.

8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet**, daß das zusätzliche, nichtflüchtige Backup-Bit über das Ladeterminal nach Abschluß des Entwertungsvorganges durch eine Sicherheitsprozedur ähnlich zu der beim Schreiben eines Freigabewertes zurückgesetzt wird.

9. Elektronische Börsenkarte für einen bargeldlosen Zahlungsverkehr mit einer integrierten Halbleiter-Schaltungsvorrichtung bestehend aus zumindest einer Adreß- und Steuerlogikschaltung und einem nichtflüchtigen Speicher, wobei zumindest ein Teil des nichtflüchtigen Speichers löschbar ist, und die Speicherplätze des zum Speichern des jeweiligen Entwertungszustandes der Börsenkarte vorgesehenen Bereiches des nichtflüchtigen Speichers in Teilbereiche (Stufen 1 bis 5) jeweils unterschiedlicher Wertigkeit (Stufenwerte 1, 8, 64, 512, 4096) aufgeteilt ist, wobei ein Löschen der Speicherplätze nur für alle Speicherplätze eines Teilbereiches bestimmter Wertigkeit gleichzeitig möglich ist, und jeder Teilbereich nur gelöscht werden kann, nachdem das Einschreiben eines Übertragwertes in eine zuvor unbeschriebene Speicherzelle des Teilbereiches der nächsthöheren Wertigkeit erfolgt ist, **dadurch gekennzeichnet**, daß
den Werteinheiten wenigstens der Speicherplätze des höchstwertigen Teilbereiches (Stufe 5) in einem Freigaberegister der Börsenkarte zu speichernde Freigabewerte zugeordnet sind, welche entweder einen Freigabe- oder einen Sperrzustand für die jeweils zugeordnete Werteinheit der Speicherplätze des wenigstens höchstwertigen Teilbereiches repräsentieren, und die Halbleiter-Schaltungsvorrichtung derart ausgebildet ist, daß eine Erhöhung des Gesamtwertes der Börsenkarte lediglich durch Änderung eines der Werteinheit eines Speicherplatzes zugeordneten Freigabewertes vom Sperr- in einen Freigabezustand ermöglicht ist.

10. Börsenkarte nach Anspruch 9, **dadurch gekennzeichnet**, daß den Speicherplätzen wenigstens des höchstwertigen Teilbereiches (Stufe 5) des Speichers ein im wesentlichen gleich aufgebautes Duplikat des Freigaberegisters zugeordnet bzw. vorgeschaltet ist.

11. Börsenkarte nach Anspruch 9 oder 10, **dadurch gekennzeichnet**, daß die Anzahl der Speicherplätze des höchstwertigen Teilbereiches (Stufe 5) des Speichers die Summe aller für die

Börsenkarte erlaubten Zahlungsvorgänge einschließlich der Aufladungen begrenzt.

12. Börsenkarte nach Anspruch 9 bis 11, **dadurch gekennzeichnet**, daß wenigstens der zum Speichern des jeweiligen Entwertungszustandes der Börsenkarte vorgesehene Bereich des nichtflüchtigen Speichers als mehrstufiger Zähler (Wertzähler) ausgebildet ist.

13. Börsenkarte nach Anspruch 12, **dadurch gekennzeichnet**, daß der mehrstufige Zähler (Wertzähler) als Oktalzähler ausgebildet ist.

14. Börsenkarte nach Anspruch 9 bis 13, **dadurch gekennzeichnet**, daß wenigstens der zum Speichern des jeweiligen Entwertungszustandes der Börsenkarte vorgesehene Bereich des nichtflüchtigen Speichers einen elektrisch löschbaren Festwertspeicher (EEPROM) aufweist.

Stufe	Wertzähler bit 7	6	5	4	3	2	1	0	Wertigkeit
5	0	0	0	0	0	0	0	0	8^4=4096
4	1	1	0	0	0	0	0	0	8^3= 512
3	1	1	0	0	0	0	0	0	8^2= 64
2	1	1	1	1	1	1	0	0	8^1= 8
1	0	0	0	0	0	0	0	0	8^0= 1

Fig 1

Stufe	Wertzähler bit 9	8	7	6	5	4	3	2	1	0	Wertstufe	Freigabezähler bit 9	8	7	6	5	4	3	2	1	0
5	1	1	1	1	1	1	1	1	1	1	8^4=4096	1	1	1	1	1	1	1	1	0	0
4			1	1	1	0	0	0	0	0	8^3= 512										
3			1	1	1	1	0	0	0	0	8^2= 64										
2			1	1	0	0	0	0	0	0	8^1= 8										
1			0	0	0	0	0	0	0	0	8^0= 1										

Fig 2.1

Stufe	Wertzähler bit 9	8	7	6	5	4	3	2	1	0	Wertstufe	Freigabezähler bit 9	8	7	6	5	4	3	2	1	0
5	1	1	1	1	1	1	1	1	0	0	8^4=4096	1	1	1	1	1	1	1	1	0	0
4			0	0	0	0	0	0	0	0	8^3= 512										
3			0	0	0	0	0	0	0	0	8^2= 64										
2			1	1	1	1	1	1	0	0	8^1= 8										
1			1	1	0	0	0	0	0	0	8^0= 1										

Fig 2.2

Stufe	Wertzähler bit 9	8	7	6	5	4	3	2	1	0	Wertstufe	Freigabezähler bit 9	8	7	6	5	4	3	2	1	0
5	1	1	1	1	1	1	1	1	0	0	8^4=4096	1	1	1	1	1	1	0	0	0	0
4			0	0	0	0	0	0	0	0	8^3= 512										
3			0	0	0	0	0	0	0	0	8^2= 64										
2			1	1	1	1	1	1	0	0	8^1= 8										
1			0	0	0	0	0	0	0	0	8^0= 1										

Fig 2.3

Stufe	Wertzähler bit 9	8	7	6	5	4	3	2	1	0	Wertstufe	Freigabezähler bit 9	8	7	6	5	4	3	2	1	0
5	1	1	1	1	1	1	1	1	0	0	8^4=4096	1	1	1	1	1	1	1	1	0	0
4			0	0	0	0	0	0	0	0	8^3= 512										
3			0	0	0	0	0	0	0	0	8^2= 64										
2			1	1	1	1	1	1	0	0	8^1= 8										
1			1	1	0	0	0	0	0	0	8^0= 1										

Fig 3.1

Stufe	Wertzähler bit 9	8	7	6	5	4	3	2	1	0	Wertstufe	Freigabezähler bit 9	8	7	6	5	4	3	2	1	0
5	1	1	1	1	1	1	1	1	0	0	8^4=4096	1	1	1	1	1	1	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	8^3= 512										
3	0	0	0	0	0	0	0	0	0	0	8^2= 64										
2	1	1	1	1	1	1	1	0	0	0	8^1= 8										
1	1	1	0	0	0	0	0	0	0	0	8^0= 1										

Fig 3.2

Stufe	Wertzähler bit 9	8	7	6	5	4	3	2	1	0	Wertstufe	Freigabezähler bit 9	8	7	6	5	4	3	2	1	0
5	1	1	1	1	1	1	1	0	0	0	8^4=4096	1	1	1	1	1	1	0	0	0	0
4	1	1	1	1	1	1	1	1	1	0	8^3= 512										
3	1	1	1	1	1	1	1	1	1	1	8^2= 64										
2	1	1	1	1	1	1	1	0	0	0	8^1= 8										
1	1	1	0	0	0	0	0	0	0	0	8^0= 1										

Fig 3.3

Stufe	Wertzähler bit 9	8	7	6	5	4	3	2	1	0	Wertstufe	Freigabezähler bit 9	8	7	6	5	4	3	2	1	0
5	1	1	1	1	1	1	1	0	0	0	8^4=4096	1	1	1	1	1	1	0	0	0	0
4	1	1	1	0	0	0	0	0	0	0	8^3= 512										
3	1	1	1	1	1	0	0	0	0	0	8^2= 64										
2	0	0	0	0	0	0	0	0	0	0	8^1= 8										
1	1	1	0	0	0	0	0	0	0	0	8^0= 1										

Fig 3.4

Stufe	Wertzähler bit 9	8	7	6	5	4	3	2	1	0	Wertstufe	Freigabezähler bit 9	8	7	6	5	4	3	2	1	0
5	1	1	1	1	1	1	1	0	0	0	8^4=4096	1	1	1	1	1	0	0	0	0	0
4	1	1	1	0	0	0	0	0	0	0	8^3= 512										
3	1	1	1	1	1	0	0	0	0	0	8^2= 64										
2	0	0	0	0	0	0	0	0	0	0	8^1= 8										
1	1	1	0	0	0	0	0	0	0	0	8^0= 1										

Fig 3.5

INTERNATIONAL SEARCH REPORT

Inte. ional Application No
PCT/EP 96/01521

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/08 G07F7/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	EP,A,0 378 454 (GEMPLUS CARD INTERNATIONAL) 18 July 1990 see abstract; claims; figures	1,9-12 3,4,14
Y	EP,A,0 345 108 (ALECTRONIQUE SERGE DASSAULT) 6 December 1989 see abstract; claims; figures	1,9-12
A	FR,A,2 608 809 (FLONIC) 24 June 1988 see abstract; claims; figures	1-4,6, 9-14
A	EP,A,0 519 847 (FRANCE TELECOM) 23 December 1992	
A	EP,A,0 646 892 (TOPPAN PRINTING) 5 April 1995	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
12 September 1996	25.09.96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Authorized officer David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. ..ional Application No
PCT/EP 96/01521

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,4 204 113 (G. GIRAUD) 20 May 1980	

1

Form PCT ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/EP 96/01521

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0378454	18-07-90	FR-A-	2641634	13-07-90
		CA-A-	2007594	11-07-90
		DE-D-	69003543	04-11-93
		DE-T-	69003543	03-02-94
		ES-T-	2047276	16-02-94
		US-A-	5264689	23-11-93
EP-A-0345108	06-12-89	FR-A-	2632101	01-12-89
		FR-A-	2639742	01-06-90
		US-A-	4992646	12-02-91
		US-A-	5030806	09-07-91
FR-A-2608809	24-06-88	AU-B-	605213	10-01-91
		AU-A-	8221887	23-06-88
		DE-A-	3777804	30-04-92
		EP-A-	0277440	10-08-88
		JP-A-	63276691	14-11-88
		US-A-	4908499	13-03-90
EP-A-0519847	23-12-92	FR-A-	2678094	24-12-92
		JP-A-	7141478	02-06-95
		US-A-	5285415	08-02-94
EP-A-0646892	05-04-95	JP-A-	7105334	21-04-95
		JP-A-	7105335	21-04-95
		JP-A-	7105336	21-04-95
		AU-A-	7434694	13-04-95
		US-A-	5504701	02-04-96
US-A-4204113	20-05-80	FR-A-	2403597	13-04-79
		CH-A-	627570	15-01-82
		DE-A-	2840325	29-03-79
		GB-A,B	2006498	02-05-79
		JP-C-	1489628	07-04-89
		JP-A-	54096339	30-07-79
		JP-B-	61018794	14-05-86

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 96/01521

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G07F7/08 G07F7/02

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G07F G06K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y A	EP,A,0 378 454 (GEMPLUS CARD INTERNATIONAL) 18.Juli 1990 siehe Zusammenfassung; Ansprüche; Abbildungen ---	1,9-12 3,4,14
Y	EP,A,0 345 108 (ALECTRONIQUE SERGE DASSAULT) 6.Dezember 1989 siehe Zusammenfassung; Ansprüche; Abbildungen ---	1,9-12
A	FR,A,2 608 809 (FLONIC) 24.Juni 1988 siehe Zusammenfassung; Ansprüche; Abbildungen ---	1-4,6, 9-14
A	EP,A,0 519 847 (FRANCE TELECOM) 23.Dezember 1992 --- -/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

1

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
12.September 1996	25. 09. 96

Name und Postanschrift der Internationale Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	David, J

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Inte. ...onales Aktenzeichen
PCT/EP 96/01521

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP,A,0 646 892 (TOPPAN PRINTING) 5.April 1995 ---	
A	US,A,4 204 113 (G. GIRAUD) 20.Mai 1980 -----	

Formblatt PCT ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Int. ..onales Aktenzeichen
PCT/EP 96/01521

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP-A-0378454	18-07-90	FR-A-	2641634	13-07-90
		CA-A-	2007594	11-07-90
		DE-D-	69003543	04-11-93
		DE-T-	69003543	03-02-94
		ES-T-	2047276	16-02-94
		US-A-	5264689	23-11-93
EP-A-0345108	06-12-89	FR-A-	2632101	01-12-89
		FR-A-	2639742	01-06-90
		US-A-	4992646	12-02-91
		US-A-	5030806	09-07-91
FR-A-2608809	24-06-88	AU-B-	605213	10-01-91
		AU-A-	8221887	23-06-88
		DE-A-	3777804	30-04-92
		EP-A-	0277440	10-08-88
		JP-A-	63276691	14-11-88
		US-A-	4908499	13-03-90
EP-A-0519847	23-12-92	FR-A-	2678094	24-12-92
		JP-A-	7141478	02-06-95
		US-A-	5285415	08-02-94
EP-A-0646892	05-04-95	JP-A-	7105334	21-04-95
		JP-A-	7105335	21-04-95
		JP-A-	7105336	21-04-95
		AU-A-	7434694	13-04-95
		US-A-	5504701	02-04-96
US-A-4204113	20-05-80	FR-A-	2403597	13-04-79
		CH-A-	627570	15-01-82
		DE-A-	2840325	29-03-79
		GB-A,B	2006498	02-05-79
		JP-C-	1489628	07-04-89
		JP-A-	54096339	30-07-79
		JP-B-	61018794	14-05-86